

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-157554

(P2002-157554A)

(43) 公開日 平成14年5月31日 (2002.5.31)

(51) Int.Cl. <sup>7</sup>	識別記号	F I	テ-マ-ト* (参考)
G 0 6 K 17/00		G 0 6 K 17/00	E 5 B 0 1 7
G 0 6 F 9/46	3 4 0	G 0 6 F 9/46	3 4 0 F 5 B 0 3 5
12/14	3 1 0	12/14	3 1 0 K 5 B 0 5 8
G 0 6 K 19/073		G 0 6 K 19/00	P 5 B 0 9 8

審査請求 未請求 請求項の数11 O L (全 14 頁)

(21) 出願番号 特願2001-220865 (P2001-220865)  
(22) 出願日 平成13年7月23日 (2001.7.23)  
(31) 優先権主張番号 特願2000-269096 (P2000-269096)  
(32) 優先日 平成12年9月5日 (2000.9.5)  
(33) 優先権主張国 日本 (J P)

(71) 出願人 000005223  
富士通株式会社  
神奈川県川崎市中原区上小田中4丁目1番1号  
(72) 発明者 栗田 享佳  
神奈川県川崎市中原区上小田中4丁目1番1号 富士通株式会社内  
(74) 代理人 100074099  
弁理士 大菅 義之 (外1名)  
Fターム(参考) 5B017 AA07 BA06 CA14  
5B035 AA13 CA11 CA29 CA38  
5B058 CA23 CA26 KA02 KA04 YA20  
5B098 AA03 GA01 GD03 GD15

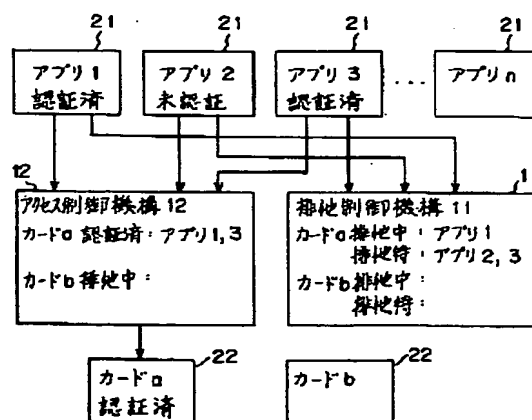
(54) 【発明の名称】 スマートカードのアクセス管理システム、共有方法及び記憶媒体

(57) 【要約】

【課題】 複数のアプリケーションによるアクセスに対し、各アプリケーション (プロセス) 毎に認証許可を与えるスマートカードのアクセス管理システム及び管理方法を提供することを課題とする。

【解決手段】 スマートカードへの複数のアクセス処理を含むアプリケーション21は、各アクセス処理毎にスマートカード22に対してアクセス要求を行う際、排他制御機構11に対して排他獲得要求を行い、排他が得られるとアクセス制御機構12に対してアクセスを要求する。アクセス制御機構12はアプリケーション21が未認証ならばPINの入力を要求し、既に認証を得られていればスマートカード22へのアクセスを許可する。アプリケーション21はアクセス処理単位で排他獲得要求/解除を行う。

排他制御機構及びアクセス制御機構を設けた場合の構成図



**【特許請求の範囲】**

【請求項1】 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードのアクセス管理システムであって、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとする排他制御手段と、

排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可するアクセス制御手段とを備えることを特徴とするアクセス管理システム。

【請求項2】 前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録することを特徴とする請求項1に記載のアクセス管理システム。

【請求項3】 前記アクセス制御手段は、前記アクセス要求に対し、前記排他を獲得したアプリケーションが前記スマートカードから未認証である時、該アプリケーションの要求を拒否することを特徴とする請求項1又は2に記載のアクセス管理システム。

【請求項4】 前記アクセス制御手段は、前記スマートカードがスマートカードリーダーより抜かれた時、該抜かれたスマートカードにより認証済みとなっているアプリケーションを未認証に変更することを特徴とする請求項1乃至3のいずれか1に記載のアクセス管理システム。

【請求項5】 前記アプリケーションは、前記スマートカードに複数回アクセスする時、各アクセスの開始時に前記排他制御手段に前記排他獲得要求を行い、該各アクセスの終了時に前記排他制御手段に排他の解除通知を行うことを特徴とする請求項1乃至4のいずれか1に記載のアクセス管理システム。

【請求項6】 前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードが他のアプリケーションによって既に排他獲得済みであれば、該排他獲得要求を行ったアプリケーションをキューに登録し、前記アプリケーションからの排他の解除通知に対し、前記キューに登録されているアプリケーションを排他獲得済みとすることを特徴とする請求項5に記載のアクセス管理システム。

【請求項7】 前記アクセス制御手段は、アプリケーションからスマートカードの認証解除の通知に対し、該認証解除が該スマートカードにより認証済みとなっている

最後のアプリケーションからの時、該スマートカードに認証解除を要求することを特徴とする請求項1乃至6のいずれか1に記載のアクセス管理システム。

【請求項8】 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードの共有方法であって、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを特徴とする共有方法。

【請求項9】 1つのスマートカードへの複数のアクセス処理を含むアプリケーション又はそのライブラリであって、

複数のアクセス処理に対し、該アクセス処理の開始時にそれぞれ排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、

前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行うことを特徴とするアプリケーション又はそのライブラリ。

【請求項10】 複数のアプリケーションが並列動作する情報処理装置によって使用された時、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを前記情報処理装置に行わせるプログラムを記憶した前記情報処理装置が読み出し可能な記録媒体。

【請求項11】 複数のアプリケーションが並列動作する情報処理装置によって実行された時、

アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許

可することを前記情報処理装置に行わせるプログラム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、スマートカード上のデータの複数プロセスによる共有した場合のスマートカードのアクセス管理に関する。

【0002】

【従来の技術】スマートカードは、従来用いられている磁気カードに比して非常に大きな容量のデータを記憶することが出来ることなどから、様々な分野への使用が検討され、あるいは実用化されている。

【0003】またスマートカードは、内部にメモリと共にCPUを備えており、このCPUを介してメモリ内のデータへアクセスを行うので、アクセス時にCPUに認証処理を行わせることにより、従来の磁気カードに比べて高いセキュリティ性を実現出来、この点もスマートカードのメリットとなっている。

【0004】スマートカードはPIN (Personal Identification Number) によるセキュリティ機能を持っており、この機能によりPINの照合を行い、認証された場合にだけカード内の秘密情報をアクセスすることができるよう制御することが可能である。このPINによる認証は、いわゆるパスワード入力方式で、スマートカードを用いるユーザがPINとして例えばパスワードを入力し、これをスマートカード内に記憶しているパスワードとカード内で比較して、一致した場合に内部データへのアクセスを許可する。

【0005】スマートカードへのアクセスは、スマートカードが持つ論理チャンネルを通して行い、認証要求は論理チャンネルに対して行われる。そしてスマートカードは、この論理チャンネル毎にPINによる認証状態などセキュリティに関する状態を保持している。

【0006】図15は、アプリケーションから見たスマートカード内部の論理的構成を示したものである。スマートカード内では、データをツリー構造の構成によって管理しており、最上位にあるDIRの下層に、使用されるアプリケーション毎の単位等でDF (Delicated File) が設けられている。そして、各DF内には実際のデータを保持しているEF (Elementary File) が格納されている。スマートカードからデータにアクセスする際、アプリケーションは、まずアクセスを行うデータの位置を示す位置付け情報を送って、目的のEFにアクセス位置を移動した後、そのEFからデータの読みだし／書込みを行う。また各チャンネルは、現在のアクセス位置を状態情報として保持している。

【0007】

【発明が解決しようとする課題】現在スマートカードを複数のアプリケーションで同時に使用する使い方が検討されている。例えば公開鍵暗号方式をベースとしたPKI (Public Key Instructure) システムを構築し、この

システム上のコンピュータで複数のアプリケーションが稼動している場合に、各アプリケーションがデジタル署名などによるセキュリティ認証にスマートカードを用いることが、現在スマートカードの1つの使用方法として考えられている。

【0008】この場合、スマートカードを接続したコンピュータ上の複数のアプリケーションがスマートカードを共用することになる。そして1つのスマートカードが持つ論理チャンネルの数はせいぜい2チャンネル程度なので、多数のアプリケーションに同一のカードに対してアクセスさせる場合、1つの論理チャンネルを複数のアプリケーションが共有する必要が出てくる。尚本明細書内の以下の説明は、説明の簡略化のため、1つのアプリケーションは1つのプロセスで構成されることを前提としており、アプリケーションという言葉のプロセスと同義で用いている。通常1つのアプリケーションは1つのプロセスで構成されることが多いが、複数のプロセスで構成されている場合でも、アプリケーションをプロセスと置換えて考えれば、以下の説明は基本的に同じである。

【0009】現行のスマートカードのセキュリティ方式では、1つのアプリケーションがある論理チャンネルに対してPIN認証を行いアクセス許可を得ると、以降その論理チャンネルからは、認証が解除されるまでの間、認証を受けたアプリケーションだけでなく他のアプリケーションもアクセス出来てしまう。

【0010】複数のアプリケーションで1つのカードの同じ情報を共有することを、セキュリティの観点から考えると、個々のアプリケーション毎にPINによる認証を行った方がセキュリティレベルはより強固になる。しかし、現行のスマートカードへのアクセス制御では、1つの論理チャンネルを複数のアプリケーションで共有する場合、論理チャンネル毎に認証が行われ各論理チャンネルに認証状態 (アクセス許可を与えたか否か) が保持されるため、1つのアプリケーションがPINによる認証を行ってアクセス許可を得れば、他のアプリケーションはPINによる認証を受けずに、その論理チャンネルからカードへのアクセスが可能となってしまう。

【0011】また、上述したように各アプリケーションは、カード内のデータにアクセスする際、位置付け情報を論理チャンネルに送信してアクセス位置を移動してからデータの書込み／読みだしを行うが、複数のアプリケーションが論理チャンネルを共有する場合、各アプリケーションはカレントのアクセス位置の把握が難しくなる。

【0012】上記問題点を鑑み、本発明は、複数のアプリケーション (プロセス) によるアクセスに対し、スマートカードへの認証状態を一元管理することにより、各アプリケーション (プロセス) 毎に認証許可を与えるスマートカードのアクセス管理システム及び管理方法を提供することを課題とする。また、各アプリケーション (プロセス) 毎の認証を認証処理によるオーバーヘッドを

大きくすること無く実現するアクセス管理システム及び管理方法を提供することを課題とする。

【0013】

【課題を解決するための手段】上記問題点を解決するため、本発明によるスマートカードのアクセス管理システムは、複数のアプリケーションによるスマートカードへのアクセスを管理するものであって、排他制御手段及びアクセス制御手段を備える。

【0014】排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとする。また上記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録する。

【0015】アクセス制御手段は、排他獲得済みとなっているアプリケーションからの上記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可する。またアクセス制御手段は、上記アクセス要求に対し、上記排他を獲得したアプリケーションが上記スマートカードから未認証である時、該アプリケーションにPINの入力を要求する。各アプリケーションによるスマートカードの認証はこのアクセス制御手段を通して行われ、アクセス制御手段は各アプリケーションとスマートカードとの認証関係を把握している。

【0016】本発明によれば、排他制御手段により、スマートカードに対する排他制御が行われるので、複数のアプリケーションによってスマートカードを共用しても各アプリケーション毎の認証を可能とする。

【0017】また、アクセス制御手段により、各アクセス要求を行ったアプリケーションが認証済みかどうか判断され、認証済みの場合、認証処理を行わずにアクセス許可を与えるので、認証処理回数を削減することが出来る。

【0018】

【発明の実施の形態】以下に本発明の一実施形態について、図面を参照しながら説明する。各アプリケーション毎に認証許可を与えるようにするためには、スマートカード（スマートカードが複数の論理チャネルをもつ場合論理チャネル）に対して排他制御を行い、認証された1つのアプリケーションがスマートカードを使用している間、そのアプリケーションがカード（若しくは論理チャネル）を専有し、他のアプリケーションからのアクセスを抑止する必要がある。尚説明簡略化の為、以下の実施

形態では各スマートカードは論理チャネルを1つ備える構成とする。尚スマートカードが複数論理チャネルを備えた場合は、以下に説明する排他制御は論理チャネル単位で行われる。

【0019】図1は、排他制御機構を設け、スマートカードにアクセスするアプリケーションの排他処理を行った場合を示す。図1では、複数のアプリケーション21とスマートカード22の間に排他制御機構11を設け、スマートカード22に対してアクセスを要求する際、各アプリケーション21はこの排他制御機構11に対して排他獲得要求を行い、排他が得られたアプリケーション21が、スマートカード22を専有してアクセスを行う。同図の排他制御機構11はカードa、bの2つのカードへのアクセスに対する排他を管理している。そしてアプリ1、アプリ2及びアプリ3の3つのアプリケーション21がカードaに対してアクセス要求を発行しており、排他制御機構11はそのうちのアプリ1に対して排他獲得とし、他のアプリ2及び3はカードaが解放されるまで待ち状態にしておく。排他を獲得したアプリ1は、カードaの論理チャネルに対してPIN認証を行った後データの読みだし/書き込みを行う。この間他のアプリケーション21は、カードaに対してアクセスすることが出来ない。アプリ1の処理を完了してカードaを解放すると、次に、待ち状態となっているアプリ2が排他を獲得し、カードaに対してPIN認証を行った後内部のデータにアクセスする。この様に排他制御機構11を設けることにより、認証を受けた1つのアプリケーションのみスマートカードに対してアクセスすることが出来る。各アプリケーション21毎の認証を実現することが出来る。

【0020】この図1の構成による方式の場合、1つのアプリケーション21がスマートカード22を使用している間このスマートカード22はこのアプリケーション21に専有されるので、他のアプリケーション21は排他が解除されスマートカード22が解放されるまで待ち状態になる。よってこの方式では、複数のアプリケーションの並列処理性能が悪く、また待ち状態にあるアプリケーションは長い期間処理を停止してハングアップした状態に見える等、非常に使い勝手が悪くなる。

【0021】これを回避するものとしては、アプリケーション21がスマートカード22へのアクセス処理が完了すると専有していたスマートカード22を逐一解放する方式がある。この方式では、アプリケーション21が複数回スマートカード22に対するアクセス処理を含む場合、各アクセス処理毎に排他制御機構11に対してスマートカード22への排他獲得/解放を行い、こまめに排他制御を区切る。

【0022】図2に、この方式による各アプリケーションのスマートカードへの排他獲得/解放の例を示す。同図は、図1と同様アプリ1、アプリ2及びアプリ3の3

つのアプリケーション21がカードaに対してアクセス要求を発行した場合の各アプリケーションのスマートカードへのアクセス処理例を示すもので、同図中排他制御機構11への矢印↑は、各アプリケーション21から排他制御機構11への排他獲得要求、排他制御機構11からの矢印↓は排他制御機構11から各アプリケーション21への排他獲得の通知を示す。また斜線部分は各アプリケーション21によるPIN認証処理、網掛け部分はスマートカード22へアクセス処理を示す。

【0023】排他を獲得したアプリケーション21が、全処理が完了するまで排他を解除してスマートカード22を解放しなかった場合、アプリ2は排他制御機構11にカードaへの排他獲得要求を行った図2中の31の位置から、既にカードaへの排他を獲得しているアプリ1が処理が完了する33の位置まで、更にアプリ3は32の位置からこのアプリ2の処理が完了するまで待ち状態となる。しかし、同図の様にアプリケーション21が各アクセス処理毎にこまめに排他制御を区切ることで、排他が解除された期間に別のアプリケーション21がカードaにアクセスすることが出来るので、排他獲得の待ち状態となり処理が停止してしまう期間が短くなり、処理の並列性が向上する。

【0024】この様に、排他制御を頻繁に切替えると、各アプリケーションの待ち状態の期間は短くなり処理の並列性は向上する。しかし図2の斜線部に示すように各アプリケーションは切替えの度に認証状態の設定／解除処理を行う必要があり、その為のオーバーヘッドが大きくなってしまふ。また認証の再許可を得る際PINを送信するので、各アプリケーション21がPINを保持し続けることになり、セキュリティ上の問題も生じる。これを回避するため、認証処理の度にユーザがパスワードを入力する構成とすると更に認証処理のオーバーヘッドが大きくなる。

【0025】図3にこの点を考慮した構成を示す。図3の構成では、複数のアプリケーション21とスマートカード22の間に、排他制御機構11に加えアクセス制御機構12を設け、このアクセス制御機構12によって各アプリケーション21のスマートカード22による認証を一元管理しながら、排他制御機構11がスマートカード22にアクセスするアプリケーション21の排他処理を行っている。

【0026】各アプリケーション21はスマートカード22に対してアクセスを要求する際、まず排他制御機構11に対して排他獲得要求を行い、排他が獲得できると次にアクセス制御機構12にスマートカード22への認証を依頼する。そして認証が得られるとスマートカード22内のデータにアクセスする。

【0027】アクセス制御機構12は認証状態管理テーブルを持ち、この認証状態管理テーブルを用いてアプリケーション21がスマートカード22への認証の開始宣

言を行ってから認証の解除を通知するまでの間について各アプリケーションとスマートカード22との認証状態の管理を行う。

【0028】図4は、認証状態管理テーブルの構成例を示す図である。認証状態管理テーブルは、各アプリケーション21が現在どのスマートカード22から認証を得ているのかを排他制御機構11が管理するために用いるテーブルで、アプリ識別情報と認証済みカード情報を対応づけて記憶している。アプリ識別情報は、各アプリケーション21を識別するための一意な識別子を記憶するもので、この識別子は、一般のアプリケーションが操作できないものが用いられ、例えばプロセス生成時に各プロセスに付加され、カーネルが管理しているプロセスIDを用いる。あるいは、スマートカードへアクセスへのアクセス要求を行ったアプリケーション21に対してアクセス制御機構12が識別子を順次生成付加してゆく構成としてもよい。

【0029】図4はカードa、bの2つのスマートカード22に対する各アプリケーション21の認証状態を管理する場合を例示しており、各アプリケーションに対し認証済みカード情報としてそのアプリケーション21が認証されているカードが記録されている。尚認証済みカード情報が空欄の部分は、そのアプリケーションに対し認証済みとなっているスマートカードが存在しないことを示す。同図では、アプリ1はカードa、b両方が認証済み、アプリ2、アプリnはいずれも未認証、アプリ3はカードaのみ認証済みとなっている。

【0030】各アプリケーション21は、スマートカード22に対する認証及びスマートカード22へのアクセスをアクセス制御機構12を介して行う。アプリケーション21からスマートカード22へのアクセス要求があると、認証状態管理テーブルを参照してそのアプリケーション21がアクセス要求したスマートカード22に認証済みであるかどうかを調べ、未認証ならばアプリケーション21からの要求を拒絶し、またアプリケーション21にPINの入力を要求してスマートカード22との認証処理を行う。また、そのアプリケーション21が認証済みならばアプリケーション21は既にそのスマートカード21の認証許可を得ているのでスマートカード21へのアクセスを許可し、実行する。

【0031】図5はアプリケーション21がスマートカード22へのアクセスを行う際の、アプリケーション21、排他制御機構11及びアクセス制御機構12の処理の流れを示した図である。同図はアプリ1がカードaに対してアクセスを行う場合を例としており、また以下の説明中の1)～23)は図5中の番号と対応している。

1) アプリ1はカードaへの排他開始を行うため、排他制御機構11に対し、排他獲得要求を行う。

2) アプリ1からの要求に対し、排他制御機構11は、カードaに対し排他獲得済のアプリケーションが有るか

調べ、既に他のアプリケーションが獲得していたならば排他待ちのキューに登録する。また排他獲得済でなければ、アプリ1に排他獲得を通知する。

3) アプリ1は、アクセス制御機構12にカードaへのアクセス開始宣言を行う。

4) アクセス開始宣言に対しアクセス制御機構12は、認証状態管理テーブルにアプリ1を登録する。そして、アプリ1にPINの入力要求を行う。尚アプリ1がカードbにもアクセス開始宣言を行っている場合は、アプリ1は既に認証状態管理テーブルに登録してあるのでカードaに対するアクセス開始宣言で再度認証状態管理テーブルに登録する必要はない。

5) アプリ1はユーザにパスワードの入力を促し、ユーザの入力からPINを指定してカードaへの認証を要求する。

6) 排他制御機構11は、カードaに対しPINを通知し、カードaに認証チェックを行わせる。

7) アクセス制御機構12は、カードaによる認証チェックの結果、認証が得られれば、認証状態管理テーブルにアプリ1がカードaに認証済みであることを登録する。

8) アプリ1はアクセス制御機構12に対し、カードaへのデータの読み出し/書き込みを要求する。

9) アプリ1からの読み出し/書き込み要求に対し、認証状態管理テーブルを検索し、アプリ1が認証済カードaに認証済みならばカードaに対してアクセスを行う。未認証ならば、アプリ1にエラーを通知する。

10) 1つのアクセス処理が完了しカードaの専有を解除する場合に、アプリ1は排他制御機構11に排他の解除を通知する。

11) 排他制御機構11は、登録されているアプリ1のカードaに対する排他獲得を削除し、他にカードaへの排他待ちのキューに登録されているアプリケーション21があればそのアプリケーション21の排他獲得を登録する。

12) 排他の解除後、アプリ1はカードaへのアクセス処理以外の処理を行う。この間、カードaの排他を解放しているので他のアプリケーション21がカードaを使用することが出来る。

13) アプリ1は、再度カードaへのアクセスの必要が生じると、排他制御機構11に排他獲得要求を行う。

14) アプリ1からの要求に対し、排他制御機構11は2)と同様、カードaに対し排他獲得済のアプリケーションが有るか再度調べ、既に他のアプリケーションが排他獲得済でなければ、アプリ1に排他獲得を通知する。

15) アプリ1はアクセス制御機構12に対し、カードaへのデータの読み出し/書き込みを要求する。

16) アクセス制御機構12は、再度9)と同様な処理を行う。この時7)で、認証状態管理テーブルにアプリ1がカードaに認証済みであることが登録されているの

で、そのままカードaへアクセスを行う。以降アプリ1内のカードaへのアクセス処理の回数分10)~16)の処理が繰り返される。

17) 全アクセス処理が完了するとアプリ1は、アクセス制御機構12にカードaへの認証を解除を通知する。

18) アクセス制御機構12は、認証状態管理テーブルのアプリ1からカードa認証済の情報を削除する。

19) アクセス制御機構12は、認証状態管理テーブル13に他にカードaに認証されているアプリケーション21が存在しなくなるまで認証状態を保持し、認証されているアプリケーション21が存在しなくなるとカードaに認証解除を要求する。これにより同一のスマートカードとの認証処理の回数を削減することが出来る。

20) アプリ1は、アクセス制御機構12にスマートカード22へのアクセス終了を通知する。

21) 20)での通知を受けるとアクセス制御機構12は認証状態管理テーブルから、アプリ1を削除する。この時アプリ1が他のスマートカード22に対してはまだアクセスを終了していない場合は認証状態管理テーブルからアプリ1を削除しない。

22) アプリ1は排他制御機構11にカードaの排他の解除を通知する。

23) 排他制御機構11は、再度11)と同様な処理を行い、排他を解除する。

【0032】図6は、図3の排他制御機構11及びアクセス制御機構12を備えた構成による各アプリケーションのスマートカードへの処理を示す図である。同図は、比較のため図2と同じ前提の元での同じアプリケーション21の処理を示してある。図6を図2と比較すると、各アプリケーション21は、認証処理としては、一番最初のカードaへのアクセス処理開始時のPINによる認証処理と、一番最後のアクセス処理終了時にカードaへの認証の解除処理を行っているのみで、図2では行っていたカードaへの各アクセス処理毎の認証処理が省略されている。よって各アプリケーション21は認証処理が省略された分処理時間が短くなる。また各アプリケーション21が、カードaを専有している期間も認証処理が省かれた分だけ短くなるので、その分待ち状態となる期間が短くてすむ可能性がある。更に各アプリケーション21は、スマートカード22に対するPIN認証を最初に1度だけ行えばよいので、カードから認証が得られればPINを破棄することが出来る。

【0033】図7は、本システムによりスマートカード22にアクセスを行うアプリケーション21の処理を示すフローチャートである。尚これらの処理を行う機構をアプリケーション21に直接持たせる構成とすることも出来るが、これらの処理をライブラリとして実現し、このライブラリを各アプリケーション21に組込む形態を取るのが一般的な構成である。

【0034】アプリケーション21は、スマートカード

22にアクセスを行う際、まず排他制御機構11へ排他獲得の依頼を行い(ステップS1)、排他制御機構11からの応答を待つ。その結果、排他制御機構11から何等かの理由で、排他が獲得出来ない旨の通知が有れば(ステップS2、NO)、処理を終了する。

【0035】排他獲得の依頼に対し、排他制御機構11から排他獲得成功の通知が有れば(ステップS2、YES)、次にステップS3として、アクセス制御機構12にスマートカード22へのアクセスの開始宣言を行う。

【0036】このスマートカード22へのアクセスが未認証のスマートカード22へのアクセスであり、スマートカード22への認証が必要なためアクセス制御機構12からPINの入力を要求された時(ステップS4、YES)、ステップS8としてPINとしてユーザが入力したパスワードをアクセス制御機構12に送って、認証処理を依頼し確認を行う。その結果認証されれば(ステップS9、YES)、処理をステップS5に移してスマートカードへアクセスし、認証されなければ(ステップS9、NO)、処理を終了する。

【0037】ステップS4において、このアクセスが既に認証を得ているスマートカード22へのアクセスである時(ステップS4、NO)、更なる認証処理は必要無いので、ステップS5としてスマートカード22へのアクセスを許可してデータの読み出し/書き込みを行う。

【0038】ステップS5のアクセス処理が終了すると、ステップS6として、アクセス制御機構12に対してスマートカード22へのアクセスの終了宣言を行う。そしてステップS7として、そのスマートカード22への排他の解除を排他制御機構11に通知してスマートカード22へのアクセス処理を終了する。

【0039】図8は、アプリケーション21からの排他獲得要求に対する排他制御機構11の処理を示すフローチャートである。アプリケーション21から、スマートカード22への排他獲得要求があると、排他制御機構11は、ステップS11として、排他獲得を要求されたスマートカード22が、既に他のアプリケーション21によって排他獲得済みであるかどうかを判断する。その結果他のアプリケーション21による排他獲得が行われていなければ(ステップS11、NO)、そのスマートカード22を排他獲得済みとして登録し、要求を行ったアプリケーション22に排他獲得を通知して処理を終了する。

【0040】またステップS11で他のアプリケーション21が排他獲得済みであるならば(ステップS11、YES)、ステップS12としてこの排他獲得要求を排他待ちキューに追加して処理を終了する。

【0041】図9は、アプリケーション21からの排他の解除通知に対する排他制御機構11の処理を示すフローチャートである。アプリケーション21からスマートカード22への排他の解除通知を受けると、排他制御機

構11は、ステップS21としてそのアプリケーション21の排他獲得済みの登録を削除して排他を解除する。

【0042】そして排他待ちキューを調べ、排他が解除されたスマートカード22に対して排他待ちとなっているアプリケーション21が存在すれば(ステップS22、YES)、排他待ちキューの先頭に登録されているアプリケーション21のそのスマートカード22への排他獲得を登録してスマートカード22をディスパッチした後、また排他待ちキューに待ちが存在しなければ(ステップS22、NO)そのまま、処理を終了する。

【0043】図10は、アプリケーション21からのスマートカード22へのアクセス要求に対するアクセス制御機構12の処理を示すフローチャートである。アプリケーション21からのアクセス開始宣言に対し、アクセス制御機構12は、ステップS31として、認証状態管理テーブルにアプリケーション21を登録して、スマートカード22に対してアクセス要求プロセスを登録する。

【0044】図11は、アプリケーション21からのスマートカード22へのアクセス要求に対するアクセス制御機構12の処理を示すフローチャートである。アプリケーション21からのアクセス要求に対し、アクセス制御機構12はステップS41として認証状態管理テーブルを参照して、そのアプリケーション21がアクセス要求先のスマートカード22から既に認証済みであるかどうか調べる。その結果、既に認証済みであれば(ステップS41、YES)、更なる認証は必要無いので、ステップS45としてアプリケーション21に対してアクセス許可を通知する。

【0045】ステップS41で、そのアプリケーション21がまだ認証を得ていないのならば(ステップS41、NO)、認証処理を行う必要があるので、ステップS42としてアプリケーション21にパスワードの入力を要求し、スマートカード22に対してPINによる認証チェックを依頼する。その結果、スマートカード22から認証が得られれば、ステップS45としてアプリケーション21に対してアクセス許可を通知し、また認証が得られなければ(ステップS43、NO)、アクセス不許可をアプリケーション21に対して通知して処理を終了する。

【0046】図12は、本実施形態に於けるスマートカードを使用するシステムの構成を示す図である。本実施形態でのアプリケーション41とスマートカード42との間を管理するアクセス管理システム40は、スマートカードリーダー43と各アプリケーション41のライブラリ44との間に構成され、OSの一機能として、あるいはOSに実装される形で実現される。

【0047】アプリケーション41は、スマートカード42に対する認証処理やアクセス処理を、全てこのアクセス管理システム40を介して行い、アクセス管理シ

テム40は、各アプリケーション41とスマートカード42との間のやり取りを把握している。またアクセス管理システム40は、スマートカードリーダ43の状態も把握しており、例えばスマートカードリーダ43からスマートカード42が抜かれると、認証状態管理テーブルを調べ、そのカードが認証済みとしているアプリケーションがあれば未認証に変更する。

【0048】なお、アクセス管理システム40は、内部に排他制御機構11とアクセス制御機構12を別々に持つ構成となっているが、これらを1つの機能構成要素として実現することもできる。また、セキュリティ上、アクセス制御機構や排他制御機構は、複数のアプリケーションが共有できる必要があるため、OSのカーネル内に実現するとセキュリティをより向上することができる。

【0049】図13は、本実施形態における上記スマートカードのアクセス管理をコンピュータプログラムにより実現した場合の情報処理装置のシステム環境図である。スマートカードを実装した情報処理装置は、図13の様にCPU51、ROM、RAMによる主記憶装置52、補助記憶装置53、ディスプレイ、キーボード等の入出力装置(I/O)54、LANやWAN、一般回線等により他の情報処理装置とネットワーク接続を行うモデム等のネットワーク接続装置55、ディスク、磁気テープなどの可搬記録媒体57から記憶内容を読み出す媒体読取り装置56及び1乃至複数のスマートカード59を実装しているスマートカードリーダ58を有し、これらが互いにバス60により接続される構成を備えている。

【0050】また図13の情報処理システムでは、媒体読取り装置56により磁気テープ、フロッピー(登録商標)ディスク、CD-ROM、MO等の記録媒体57に記憶されているプログラム、データを読み出し、これを主記憶装置52またはハードディスク55にダウンロードする。そして本実施形態による各処理は、CPU51がこのプログラムやデータを実行することにより、ソフトウェア的に実現することが可能である。

【0051】また、この情報処理装置では、フロッピーディスク等の記録媒体57を用いてアプリケーションソフトの交換が行われる場合がある。よって、本発明は、スマートカードのアクセス管理システムや共有方法に限らず、コンピュータにより使用されたときに、上述の本発明の実施の形態の機能をコンピュータに行わせるためのコンピュータ読み出し可能な記録媒体57として構成することもできる。

【0052】この場合、「記録媒体」には、例えば図14に示されるように、CD-ROM、フロッピーディスク(あるいはMO、DVD、リムーバブルハードディスク等であってもよい)等の媒体駆動装置77に脱着可能な可搬記録媒体76や、ネットワーク回線73経由で送信される外部の装置(サーバ等)内の記憶手段(データ

ベース等)72、あるいは情報処理装置71の本体74内のメモリ(RAM又はハードディスク等)75等が含まれる。可搬記録媒体76や記憶手段(データベース等)72に記憶されているプログラムは、本体74内のメモリ(RAM又はハードディスク等)75にロードされて、実行される。

【0053】(付記1) 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードのアクセス管理システムであって、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとする排他制御手段と、排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可するアクセス制御手段とを備えることを特徴とするアクセス管理システム。

【0054】(付記2) 前記排他制御手段は、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在しなければ、該排他獲得要求を行ったアプリケーションをキューに登録することを特徴とする付記1に記載のアクセス管理システム。

【0055】(付記3) 前記アクセス制御手段は、前記アクセス要求に対し、前記排他を獲得したアプリケーションが前記スマートカードから未認証である時、該アプリケーションの要求を拒絶することを特徴とする付記1又は2に記載のアクセス管理システム。

【0056】(付記4) 前記アクセス制御手段は、アプリケーションとスマートカードとの認証関係を該アプリケーションのプロセスIDを用いて管理することを特徴とする付記1乃至3のいずれか1に記載のアクセス管理システム。

【0057】(付記5) 前記アクセス制御手段は、前記スマートカードがスマートカードリーダより抜かれた時、該抜かれたスマートカードにより認証済みとなっているアプリケーションを未認証に変更することを特徴とする付記1乃至4のいずれか1に記載のアクセス管理システム。

【0058】(付記6) 前記アプリケーションは、前記スマートカードに複数回アクセスする時、各アクセスの開始時に前記排他制御手段に前記排他獲得要求を行い、該各アクセスの終了時に前記排他制御手段に排他の解除通知を行うことを特徴とする付記1乃至5のいずれか1に記載のアクセス管理システム。

【0059】(付記7) 前記排他制御手段は、アプリ



ケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードが他のアプリケーションによって既に排他獲得済みであれば、該排他獲得要求を行ったアプリケーションをキューに登録し、前記アプリケーションからの排他の解除通知に対し、前記キューに登録されているアプリケーションを排他獲得済みとすることを特徴とする付記6に記載のアクセス管理システム。

【0060】(付記8) 前記アクセス制御手段は、アプリケーションからスマートカードの認証解除の通知に対し、該認証解除が該スマートカードにより認証済みとなっている最後のアプリケーションからの時、該スマートカードに認証解除を要求することを特徴とする付記1乃至7のいずれか1に記載のアクセス管理システム。

【0061】(付記9) 複数のアプリケーションによるスマートカードへのアクセスを管理するスマートカードの共有方法であって、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、排他獲得済みとなっているアプリケーションからの前記スマートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを特徴とする共有方法。

【0062】(付記10) 1つのスマートカードへの複数のアクセス処理を含むアプリケーション又はそのライブラリであって、複数のアクセス処理に対し、該アクセス処理の開始時にそれぞれ排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行うことを特徴とするアプリケーション又はそのライブラリ。

【0063】(付記11) 1つスマートカードへの複数のアクセス処理を含むアプリケーションのライブラリであって、複数のアクセス処理に対し、該アクセス処理の開始時にそれぞれ排他獲得要求を行い、各アクセス処理の終了時にそれぞれ排他の解除通知し、前記複数のアクセス処理のうちの最初の処理時のみに該アクセス処理を行うスマートカードに対して認証要求を行うことを特徴とするアプリケーションのライブラリ。

【0064】(付記12) 複数のアプリケーションが並列動作する情報処理装置によって使用された時、アプリケーションからのスマートカードに対する排他獲得要求に対し、該スマートカードに他のアプリケーションによって排他獲得済みとなっていない論理チャネルが存在すれば、該アプリケーションを排他獲得済みとし、排他獲得済みとなっているアプリケーションからの前記スマ

ートカードへのアクセス要求に対し、該排他獲得済みとなっているアプリケーションが該スマートカードから既に認証されている時、該排他獲得済みとなっているアプリケーションに該スマートカードへのアクセスを許可することを前記情報処理装置に行わせるプログラムを記憶した前記情報処理装置が読み出し可能な記録媒体。

【0065】

【発明の効果】本発明によれば、スマートカードに対する排他制御が行われるので、複数のアプリケーションによってスマートカードを共用しても各アプリケーション単位の認証を可能とする。

【0066】また、各アプリケーションとスマートカードとの間の認証関係が一元管理されているので、アプリケーションがスマートカードにアクセス要求を行うとそのスマートカードはそのアプリケーションを認証済みかどうか判断され、未認証の場合のみ認証処理が行われるので、認証処理回数を削減することが出来、認証処理によるオーバーヘッドを小さくすることが出来る。またPINによる認証処理は、最初に一度だけ行われるのでアプリケーションは、PINを保持し続ける必要がなく、セキュリティレベルの向上が図れる。

【0067】更にスマートカードは、認証状態を保持したまま複数の認証済みアプリケーションとの間でアクセスが可能となる。またアプリケーションは、排他獲得の待ち状態期間を短く出来る。よって処理の並列性を向上出来また各アプリケーションの処理時間の短縮を図れる。

【図面の簡単な説明】

【図1】排他制御機構を設け、スマートカードへのアクセスの排他処理を行った場合の構成を示す図である。

【図2】排他制御機構を備えた構成時の各アプリケーションのスマートカードへのアクセス処理を示す図である。

【図3】排他制御機構及びアクセス制御機構を設けた場合の構成図である。

【図4】認証状態管理テーブルの構成例を示す図である。

【図5】アプリケーションがスマートカードへのアクセスを行う際の、アプリケーション、排他制御機構及びアクセス制御機構の処理の流れを示した図である。

【図6】排他制御機構及びアクセス制御機構を備えた構成時の各アプリケーションのスマートカードへのアクセス処理を示す図である。

【図7】スマートカードにアクセスを行うアプリケーションの処理を示すフローチャートである。

【図8】アプリケーションからの排他獲得要求に対する排他制御機構の処理を示すフローチャートである。

【図9】アプリケーションからの排他の解除通知に対する排他制御機構の処理を示すフローチャートである。

【図10】アプリケーションからのスマートカードへの

アクセス開始宣言に対するアクセス制御機構の処理を示すフローチャートである。

【図11】アプリケーションからのスマートカードへのアクセス要求に対するアクセス制御機構の処理を示すフローチャートである。

【図12】本実施形態に於けるスマートカードを使用するシステムの構成を示す図である。

【図13】情報処理装置のシステム環境図である。

【図14】記憶媒体の例を示す図である。

【図15】スマートカード内部の論理的構成を示す図である。

【符号の説明】

11 排他制御機構

12 アクセス制御機構

21、41 アプリケーション

22、42、59 スマートカード

40 アクセス管理システム

43、58 スマートカードリーダー

51 CPU

52 主記憶装置

55 補助記憶装置

54 入出力装置

55 ネットワーク接続装置

56 媒体読取り装置

57 可搬記憶媒体

60 バス

71 情報処理装置

72 記憶手段

73 ネットワーク回線

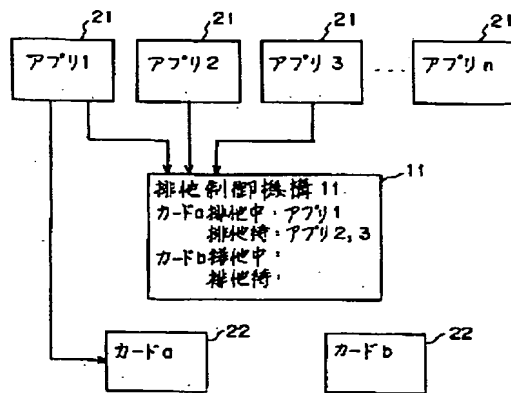
74 情報処理装置本体（コンピュータ）

75 メモリ

76 可搬記録媒体

【図1】

排他制御機構を設け、スマートカードへのアクセスの排他処理を行った場合の構成を示す図



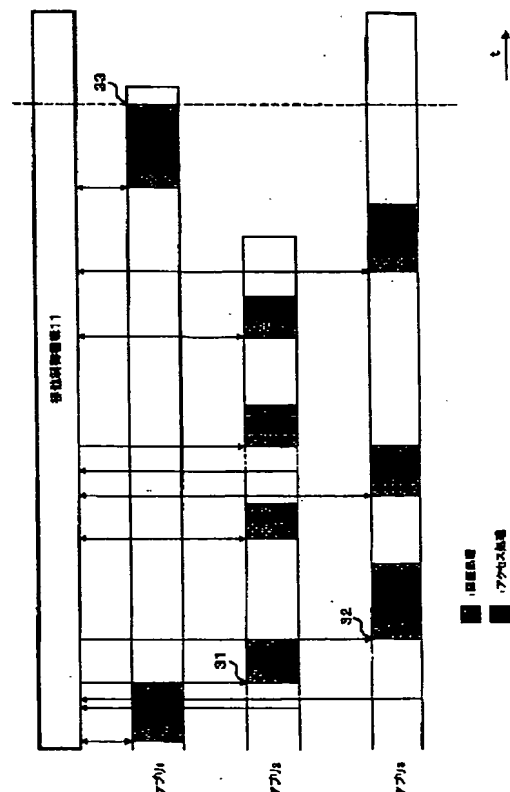
【図4】

認証状態管理テーブルの構成例を示す図

アプリ識別情報	認証済みカード情報	
アプリ1	カードa	カードb
アプリ2		
アプリ3	カードa	
.....	.....	.....
アプリn		

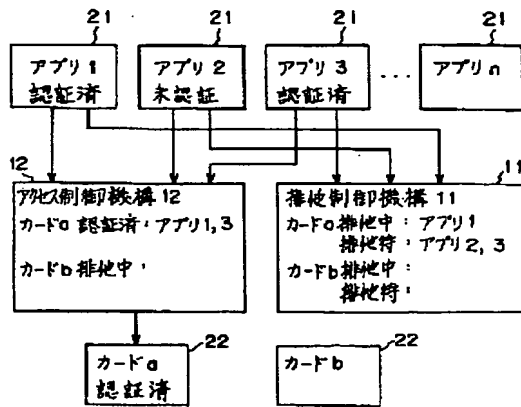
【図2】

排他制御機構を備えた構成時の各アプリケーションへのスマートカードへのアクセス処理を示す図



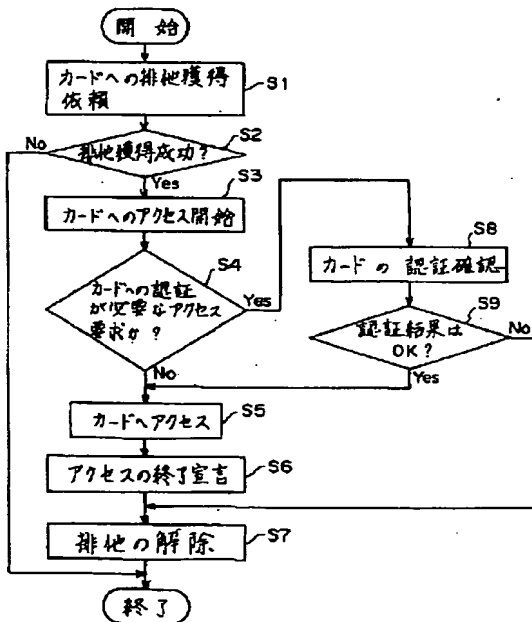
【図3】

排他制御機構及びアクセス制御機構を  
設けた場合の構成図



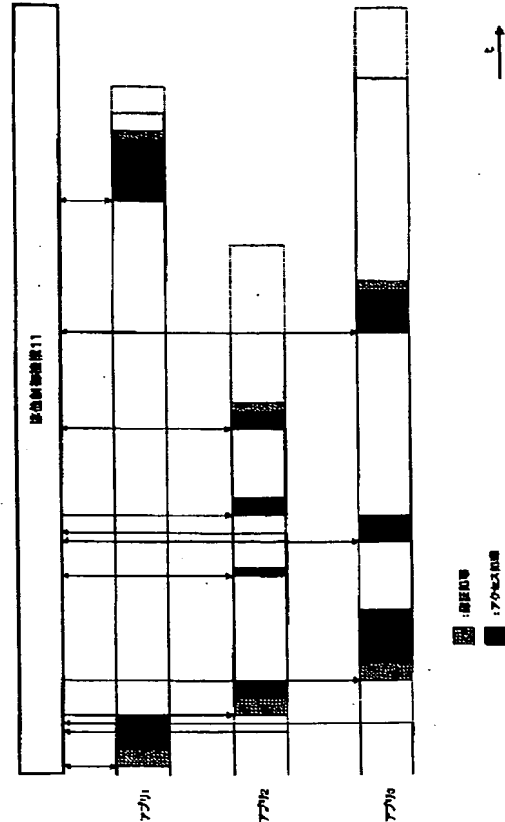
【図7】

スマートカードにアクセスを行うアプリケーションの  
処理を示すフローチャート



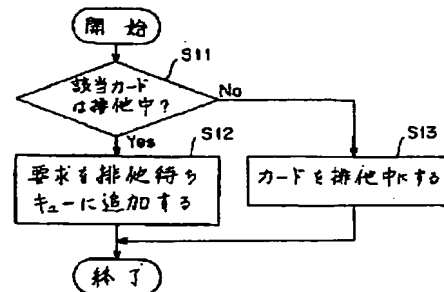
【図6】

排他制御機構及びアクセス制御機構を備えた構成時の  
各アプリケーションへのスマートカードへのアクセス処理を示す図



【図8】

アプリケーションからの排他獲得要求に対する  
排他制御機構の処理を示すフローチャート



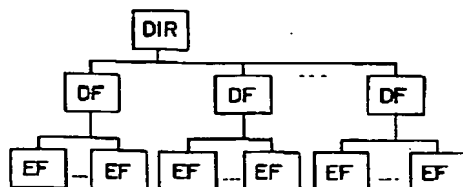
【図5】

アプリケーションがスマートカードへのアクセスを行う際の、アプリケーション、  
排他制御機構及びアクセス制御機構の処理の流れを示した図



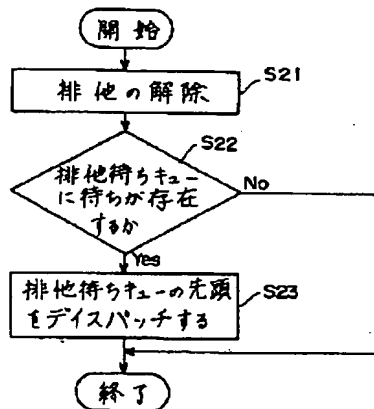
【図15】

スマートカード内部の論理的構成を  
示す図



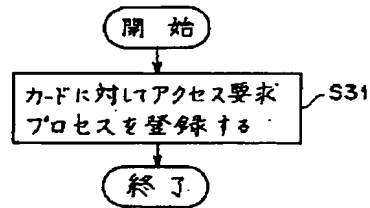
【図9】

アプリケーションからの排他解除通知に対する排他制御機構の処理を示すフローチャート



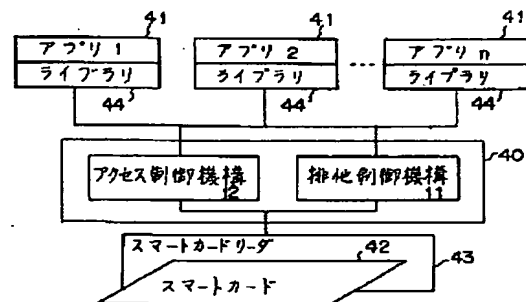
【図10】

アプリケーションからのスマートカードへのアクセス開始宣言に対するアクセス制御機構の処理を示すフローチャート



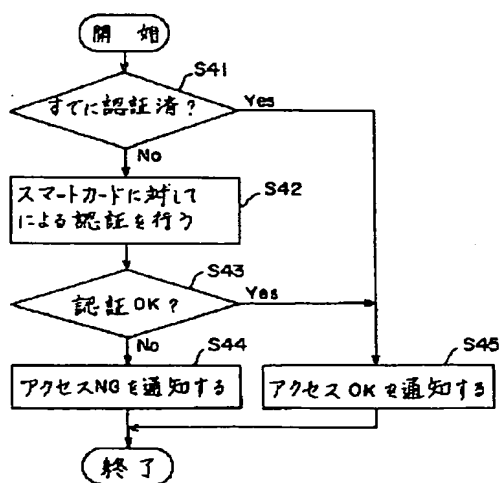
【図12】

本実施形態におけるスマートカードを使用するシステムの構成を示す図



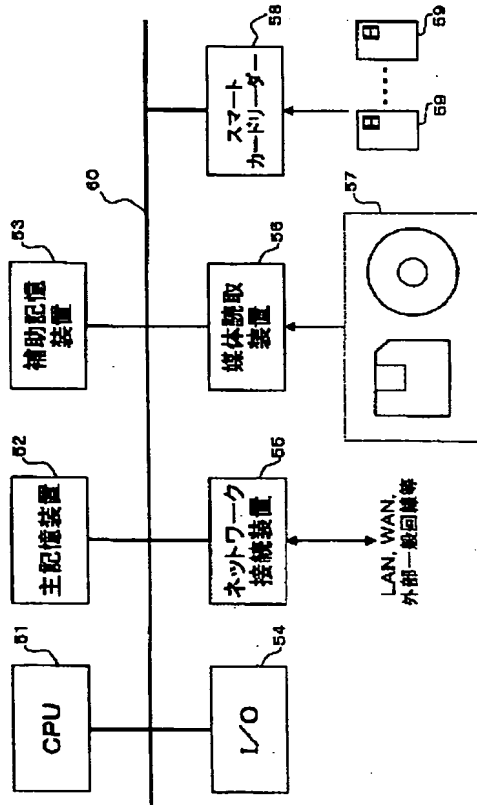
【図11】

アプリケーションからのスマートカードへのアクセス要求に対するアクセス制御機構の処理を示すフローチャート



【図13】

情報処理のシステム環境図



【図14】

記憶媒体の例を示す図

